UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/596,863	03/12/2007	Luis Ramos Robles	P18230-US1	1476

27045 7590 11/18/2009

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
11/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/596,863	RAMOS ROBLES ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 October 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *30-32 and 46-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *30-32 and 46-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *6/27/06* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **10/7/09** has been entered.

Claims 30-32 and 46 are amended. Claims 30-32 and 46-49 are pending.

Response to Amendment

Drawings

The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the subject matter entered by amendment to claims 31 and 32 must be shown or the feature(s) canceled from the claim(s). The drawings do not show a second user and the matching checks. No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended

replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

Claim 1 is objected to because of the following informalities:

"a session at the access level" in the last limitation should be "the access session" as defined in the second to last limitation.

Response to Arguments

Applicant's arguments filed 9/16/09 have been fully considered but they are not persuasive. In response to applicant's argument that the references fail to show certain

features of applicant's invention, it is noted that the features upon which applicant relies (i.e., explaining the SSO mechanism and connecting SSO to HTTP) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The prior art of Costa teaches using a shared secret K and client identification information gained during an initial authentication process whereby the first service provider [SSO manager] lends the client's authentication validation to another service provider (0048-0050). The first service provider acts as the SSO manager because it provides SSO functionality to the user/client device. Also the authentication server 134 of Figure 1 acts to provide authentication information to service providers on behalf of the client device once said client device has authenticated with said authentication server. This allows the client device to take part in authentication protocols that it does not natively support (0034).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 30-32, 46, 48, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP Application Publication 2004/0225878 to Costa-Requena et al.,

hereinafter Costa in view of publication by Cisco "ITP MAP Gateway for Public WLAN SIM Authentication and Authorization" hereinafter Cisco. This publication was published no later than Sep. 8, 2003 as it was used as a reference and cited to have been downloaded from Cisco website on said date for USP 7,536,464. Copies of those findings are provided on the last two pages of the Cisco reference.

As per claim 30, Costa teaches an apparatus comprising:

An authentication gateway operable to receive an access request in a telecommunication core network sent by a user equipment of a user, the user being a subscriber of the telecommunication CN and being identified by a user's identifier included in the access request,

the authentication gateway operable to carry out an authentication procedure with the UE in order to authenticate the user (0034); by computing at least one secret user's key usable as cryptograph material [EAP; calculations are inherently performed on the Ki secret key employed by the GSM standard; (0029, 0052)];

the apparatus further comprising:

a means for deriving from the cryptographic material a user's shared key (shared secret key; 0048) intended for SSO purposes (0050); and

a means for sending the user's shared key along with the user's identifier towards a SSO session manager serving a service network of a mobile network operator (0050) wherein the SSO session manager is operable to manage a session record for a user accessing the service network through an access network (0050).

the authentication gateway further being operable to receive a notification that an access session has been established , the notification triggering the sending of the user's shared key towards the SSO session manager; the authentication gateway being further operable to receiving a notification that a session at the access level has been terminated, and forwarding the termination notification [federation terminal notification protocol] towards the SSO session manager in order to inactivate a current master session for the user [the SSO manager (324) is part of the authentication server (134), (claim's authentication gateway), Costa teaches the authentication server employs authentication by whatever protocol is required (0054); the SSO manager (liberty manager) is able to know whether or not the user has already been authenticated (0050); this proves inherent notification between the authentication server and SSO manager; in order for SSO to work it must only provide authentication for the user when the session is active].

Costa teaches the user can be authenticated in a network independent of the device or protocol. Costa teaches many types of authentication including WLAN (0045, IMS/AKA (0048), EAP (0049), etc. Basically any device with an IP can be authenticated by the authentication server. Costa teaches both WLAN access (142,144 of Figure 1) and GSM/SIM access for mobile phones (132 of Figure 1). Costa does not explicitly teach authentication wherein the subscribing user connects through a WLAN to the telecommunication core network. Cisco teaches this limitation and structure by authenticating GSM/SIM based phones connecting through a WLAN to their respective telecommunication network (see page 2 and figure 6). Cisco teaches it is possible to

seamlessly combine the GSM authentication architecture through a public WLAN. This allows a subscriber to access the core network anywhere he/she can get onto an IP LAN yet still provides security over a public network. This increase in network availability is desirable. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the WLAN/GSM merger of Cisco within the ALL-IP based authentication system of Costa because it would expend the network availability to the connecting users.

As per claim 31, Costa teaches receiving a first user's shared key (0048) and a user's identifier (0049) from the core network for SSO authentication purposes (0050), the first user's shared key obtainable during the authentication of the user by the core network;

means for creating a master session for the user that comprises the user's identifier and the received first user's shared keys and means for checking whether a second user's shared key derived at the user's equipment matches the first user's shared key included in the master session for the user [interpreted as a request for authentication matches the first authentication token, thereby proving the same user is requesting SSO service (0050)].

As per claim 32, Costa teaches creating a service session to index a master session, in case of matching first and second user's shared keys, the service session being a token of a successful SSO user authentication [interpreted as a request for

authentication matches the first authentication token, thereby proving the same user is requesting SSO service (0050)].

As per claim 46, Costa teaches a user equipment usable by a user with a subscription in a telecommunication network comprising:

Means for accessing a service network of a mobile network operator through a wireless local access network,

means for carrying out an authentication procedure to authenticate the user with a core network (GSM; 0029), wherein the authentication gateway is operable to receive notifications that an access session has been established and terminated (0049);

means for computing at least one secret user's key (calculations are inherently performed on the Ki secret key employed by the GSM standard; 0029, 0048 0052) usable as cryptographic material,

a means for deriving from the cryptographic material a user's shared key intended for SSO purposes (0035, 0048, and 0050);

a repository for storing the user's shared key (0035; SIM); and

a means for confirming to SSO session manager of the MNO-SN the user's shared key stored at the user's equipment (0048 and 0050).

Costa teaches the user can be authenticated in a network independent of the device or protocol. Costa teaches many types of authentication including WLAN (0045, IMS/AKA (0048), EAP (0049), etc. Basically any device with an IP can be authenticated by the authentication server. Costa teaches both WLAN access (142,144 of Figure 1)

and GSM/SIM access for mobile phones (132 of Figure 1). Costa does not explicitly teach authentication wherein the subscribing user connects through a WLAN to the telecommunication core network. Cisco teaches this limitation and structure by authenticating GSM/SIM based phones connecting through a WLAN to their respective telecommunication network (see page 2 and figure 6). Cisco teaches it is possible to seamlessly combine the GSM authentication architecture through a public WLAN. This allows a subscriber to access the core network anywhere he/she can get onto an IP LAN yet still provides security over a public network. This increase in network availability is desirable. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the WLAN/GSM merger of Cisco within the ALL-IP based authentication system of Costa because it would expend the network availability to the connecting users.

As per claim 48, Costa teaches a means for confirming to a session manager of the MNO-SN the user's shared key includes a means for processing the user's shared key to obtain a key code [integrity check] to be transmitted to the session manager of the MNO-SN in the service network (0048).

As per claim 49, Costa teaches means for receiving an SSO cookie [security token] from the session manager of the MNO-SN, the SSO cookie to be included in all further service requests from the user's equipment as an SSO token (0034).

Claim 47 is rejected under 35 U.S.C. 103(a) as being unpatentable over Costa and Cisco as applied to claim 46 and in further view of publication “Using GSM/UMTS for Single Sign-On" by Pashalidis and Mitchell hereinafter Mitchell.

As per claim 47, Costa and Cisco are silent in disclosing means for confirming includes a means for downloading an SSO plug-in from an entity in the service network, the SSO plug-in running for confirming back the user's shared key. Mitchell’s system of a single sign-on mechanism through a SIM based phone teaches that the protocol can be implement in a continuously running process (AKA 'service' or ‘daemon') to minimized the user’s interaction (see page 141, last paragraph before section 4). The service running in the background would keep the user authenticated if the system requires him/her to ever re-authenticate. It would also allow the system to know that the user was still active in the network therefore not time-out the user. It would be beneficial to the Costa and Cisco system to implement this feature because it would lessen the burden and interaction required by the user to stay authenticated in the network. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine this feature of Mitchell within the system of Costa and Cisco to minimize the burden of the user to stay connected in the network.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is

(571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431